



Zpracování osobních údajů pro službu Magenta EDR

Platné od 1.10.2024

1 Podmínky zpracování osobních údajů pro službu Magenta EDR

- 1.1. Ukládání a jiné zpracování dat, která mají charakter osobních údajů ve smyslu nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, (dále jen „GDPR“) a zákona č. 110/2019 Sb., o zpracování osobních údajů, v platném znění (dále jen „Zákon o zpracování osobních údajů“) (dále společně jako „Applikovatelné právo“), v rámci služby Magenta EDR (dále jen „Služba“) se řídí níže uvedenými podmínkami.
- 1.2. V rámci Služby může docházet ke zpracování osobních údajů fyzických osob, např. zákazníků, zaměstnanců zákazníků (dále jen „**Subjekty údajů**“). Smluvní partner (dále také jen „Správce“) je při zpracování osobních údajů v souladu s ustanovením článku 4 bodu 7 GDPR v postavení správce osobních údajů. Poskytovatel (dále také jen „Zpracovatel“) je v souladu s ustanovením článku 4 bodu 8 GDPR v postavení zpracovatele osobních údajů.
- 1.3. Nedílnou součástí podmínek je Příloha č. 1 – *Technická a organizační opatření upravující zabezpečení osobních údajů*, Příloha č. 2 – *Specifikace zpracování* a Příloha č. 3 – *Schválení Dílčí zpracovatelé a Subdodavatelé Dílčích zpracovatelů*.

Zpracování osobních údajů

- 1.4. Správce pověřuje Zpracovatele zpracováním osobních údajů a Zpracovatel tyto údaje bude zpracovávat výhradně za účelem zajištění plnění Služby na základě Specifikace služby Magenta EDR (dále jen „Specifikace služby“) poskytované v rámci Smlouvy o Firemním řešení/ Smlouvy o poskytování veřejně dostupné služby elektronických komunikací. Zpracovatel zpracovává osobní údaje vždy transparentně, korektně, pouze v nezbytném rozsahu, po nezbytnou dobu a v souladu s Applikovatelným právem. Zpracovatel nepoužije osobní údaje k žádnému jinému účelu a neposkytne je žádným neoprávněným třetím stranám. Bez souhlasu Správce nesmí být pořizovány kopie a duplikáty osobních údajů – to neplatí v případě provádění záloh k zajištění řádného zpracovávání osobních údajů a/nebo řádnému poskytování Služby nebo činnosti k zajištění důvěrnosti, integrity, dostupnosti a odolnosti systémů Zpracovatele nebo plnění zákonné povinnosti.
- 1.5. Předmětem zpracování jsou osobní údaje předávané Zpracovateli prostřednictvím nebo v souvislosti s poskytovanou Službou v souladu se Specifikací služby, tj. pro ochranu vybraných koncových zařízení IT systémů (chráněných zařízení) a analýzu bezpečnostních událostí identifikovaných v IT systémech Smluvního partnera. O rozsahu zpracováváných osobních údajů rozhoduje Správce. Zpracovatel zpracovává data z provozu zařízení za účelem poskytování služby. Jsou zpracovávána zejména metadata o spuštěných souborech, vykonaných příkazech, síťových spojení, přihlášených uživatelích. Podmínky zpracování na Bezpečnostní platformě se řídí podmínkami výrobce Bezpečnostní platformy a agenta uvedenými na: <https://www.crowdstrike.com/privacy-notice/>

Poskytovatel dále zpracovává osobní údaje uživatelů určených Smluvním partnerem za účelem zajištění komunikace se zástupci Smluvního partnera. Poskytovatel v tomto případě zpracovává osobní údaje v následujícím rozsahu: jméno, pracovní pozice, telefonní číslo, e-mailová adresa.
- 1.6. Správce odpovídá za to, že osobní údaje, které jsou předmětem zpracování, jsou přesné, byly shromážděny v souladu s právními předpisy, zejména v souladu s GDPR a zákonem o zpracování osobních údajů.
- 1.7. Správce nese výhradní odpovědnost za posouzení, zda lze osobní údaje zpracovávat v souladu s platnou právní úpravou v oblasti ochrany osobních údajů, zejména v souladu s Applikovatelným právem, jakož i za ochranu práv subjektů údajů, a to zejména tak, aby Zpracovatel mohl poskytovat Služby dohodnutým způsobem, který není v rozporu s právními předpisy. Správce se zavazuje informovat Zpracovatele o jakémkoliv podezření, které může mít vliv na poskytovanou Službu.
- 1.8. Zpracovatel se zavazuje zpracovávat osobní údaje pouze na základě těchto Podmínek a doložených písemných pokynů Správce. Pro vyloučení pochybností ze zpracování osobních údajů v souladu s povinnostmi Zpracovatele vyplývajícími ze Specifikace služby považuje za zpracování prováděné v souladu s instrukcemi Správce, resp. Správcem k tomu pověřených osob. Pokud je určitý pokyn podle názoru Zpracovatele nezákonným, bez zbytečného odkladu o tom informuje Správce. V takovém případě je oprávněn pozastavit plnění pokynu.
- 1.9. Zpracovatel zpracovává osobní údaje zejména automatizovaným způsobem a v nezbytných případech manuálně.

Zabezpečení osobních údajů

- 1.10. Správce a Zpracovatel jsou povinni přijmout veškerá vhodná technická a organizační opatření, aby zajistili úroveň ochrany odpovídající riziku a poskytované Službě. Opatření Zpracovatele, která jsou v současné době pokládána za adekvátní, jsou popsána v Příloze č. 1 – *Technická a organizační opatření upravující zabezpečení osobních údajů*. Jakékoli pokyny nebo opatření, které představují odchylku od zde uvedených opatření, se skládají za žádost o úpravu, jejíž náklady, pokud budou úpravy technicky realizovatelné a možné, nese Správce. Smluvní Strany v takovém případě uzavřou samostatnou dohodu o rozsahu činnosti, výši a úhradě nákladů.
- 1.11. Zpracovatel přijal a udržuje adekvátní technická a organizační opatření, aby nedošlo k neoprávněnému nebo nahodilému přístupu k osobním údajům Správce, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů, a to s přihlédnutím k poskytované Službě.
- 1.12. Zpracovatel je oprávněn prokázat plnění závazků, zejména potom technických a organizačních opatření, prostřednictvím následujících nástrojů: a) Kodexem chování (čl. 40 GDPR); b) Závaznými podnikovými pravidly; c) Osvědčením (čl. 42 GDPR); d) aktuálními certifikáty, zprávami nebo výpisy ze zpráv od nezávislých instancí (např. auditorů, oddělení auditu); d) vhodnou certifikací ve formě auditu bezpečnosti IT nebo ochrany údajů; e) čestnými prohlášeními Zpracovatele.
- 1.13. Zpracovatel je povinen bez zbytečného odkladu informovat Správce o jakýchkoli případech porušení zabezpečení Údajů, a to na e-mailovou adresu Kontaktní osoby (ADSR) uvedenou ve Specifikaci služby.

Povinnost mlčenlivosti

- 1.14. Zpracovatel zajistí, že každá osoba, která bude mít přístup k osobním údajům, bude zavázána povinností mlčenlivosti nebo se na ni bude vztahovat zákonná povinnost mlčenlivosti. Povinnost mlčenlivosti trvá rovněž po ukončení hlavní smlouvy.

Poskytování součinnosti

- 1.15. Zpracovatel bude s přihlédnutím k charakteru zpracování a k informacím, kterými Zpracovatel disponuje, poskytovat Správci součinnost při plnění povinností Správce dle Applikovatelného práva.



1.16. Zpracovatel je povinen zajistit součinnost v následujících bodech:

- 1.16.1. Správce je oprávněn na vlastní náklady prověřovat soulad s plněním povinností dle smlouvy o zpracování osobních údajů a čl. 28 GDPR (povinnosti zpracovatele osobních údajů). Zpracovatel umožní Správci na jeho žádost, ne však častěji než 1x za kalendářní rok, vykonat kontrolu či audit. Správce se zavazuje oznamovat kontroly s přiměřeným předstihem, minimálně 30 (třicet) pracovních dnů předem, aby byla ze strany Zpracovatele zajištěna dostatečná součinnost. Správce je povinen kontroly provádět pouze v rozsahu nezbytně nutném pro ověření plnění ve vztahu ke zpracování osobních údajů pro jemu konkrétně poskytovanou Službu, a pouze pokud mu Zpracovatel nedoloží plnění závazků: a) Kodexem chování (čl. 40 GDPR); b) Závaznými podnikovými pravidly; c) Osvědčením (čl. 42 GDPR); d) aktuálními certifikáty, zprávami nebo výpisy ze zpráv od nezávislých instancí (např. auditorů, oddělení auditu); e) vhodnou certifikací ve formě auditu bezpečnosti IT nebo ochrany údajů; e) čestnými prohlášeními Zpracovatele, a vždy tak, aby nenarušoval běžnou činnost Zpracovatele a byla zachována důvěrnost. Správce nemůže mít přístup k informacím, které jsou předmětem obchodního tajemství Zpracovatele. Zpracovatel je zároveň oprávněn podmínit umožnění kontroly či auditu uzavřením zvláštní dohody o ochraně důvěrnosti informací a dodržením předem sdělených interních pravidel Zpracovatele.
- 1.16.2. Pokud je Správce povinen poskytnout orgánům státní správy nebo osobám informace o zpracovávání osobních údajů, Zpracovatel poskytne Správci při poskytování takových informací součinnost, pokud se tyto informace týkají zpracovávání údajů v souladu se Specifikací služby a poskytovanou Službou. Zpracovatel rovněž Správce vyrozumí – pokud to zákon připouští – o jakýchkoli sděleních dozorových orgánů (např. šetření, oznámení o opatřeních nebo požadavcích) Zpracovateli v souvislosti se zpracováváním osobních údajů podle Specifikace služby.
- 1.16.3. Zpracovatel je povinen poskytnout Správci součinnost ve vztahu k povinnosti Správce reagovat na žádost o uplatnění práv subjektů údajů dle čl. 15 až 22 GDPR, a to v rozsahu, v němž je to s ohledem na podmínky příslušné Služby a technické a organizační podmínky možné. V případě potřeby budou smluvní strany koordinovat obsah a rozsah činnosti ve formě podpory poskytované Zpracovatelem podle tohoto odstavce. Pokud se Subjekt údajů obrátí přímo na Zpracovatele a z podání bude možné určit, že se žádost týká Správce, Zpracovatel žádosti Subjektu údajů bezodkladně postoupí Správci.
- 1.16.4. Zpracovatel je povinen poskytnout na základě žádosti Správce odeslané na Zákaznické centrum T-Mobile (nejméně 10 pracovních dnů předem) informace potřebné k doložení plnění povinností Zpracovatele dle článku 28 GDPR (povinnosti zpracovatele osobních údajů).
- 1.16.5. Zpracovatel je povinen poskytovat na základě žádosti Správce odeslané na Zákaznické centrum T-Mobile (nejméně 10 pracovních dnů předem) součinnost při zajišťování souladu s povinnostmi Správce dle článků 32 a 36 GDPR, a to při zohlednění povahy zpracování a informací, jež má Zpracovatel od Správce k dispozici.
- 1.16.6. Pokud Správce provede posouzení dopadu na ochranu soukromí (osobních údajů) a/nebo konzultace s dozorovým orgánem k posouzení dopadu na ochranu soukromí, smluvní strany budou koordinovat obsah a rozsah případné podpory poskytované Zpracovatelem, bude-li nutná.

- 1.17. Výše uvedené činnosti Zpracovatele podle bodu 1.16 jdou na náklad Správce a hradí se zvlášť podle časové náročnosti nebo využitých prostředků, a to zpětně za měsíc, ve kterém byla Správci poskytnuta, podle čl. 2 těchto Podmínek.

Pověřenec pro ochranu osobních údajů

- 1.18. Zpracovatel se zavazuje ustanovit nezávislého, kvalifikovaného a spolehlivého Pověřence pro ochranu osobních údajů, pokud to vyžadují právní předpisy Evropské unie nebo členského státu, které se na Zpracovatele vztahují.

Předávání do třetích zemí

- 1.19. V případě, že by ze strany Zpracovatele docházelo k předání osobních údajů do tzv. třetích zemí (tj. zemí, které nejsou členskými státy Evropské unie a nedisponují patřičnou úrovní ochrany osobních údajů) nebo mezinárodní organizace, Zpracovatel bude zpracovávat osobní údaje v souladu s příslušnými právními předpisy Evropské unie. V takovém případě Zpracovatel předem informuje Správce, ledaže by takové informování právní předpisy zakazovaly z důležitých důvodů veřejného zájmu.

Dílčí zpracovatelé

- 1.20. Zpracovatel nezapojí do zpracování osobních údajů žádného dalšího zpracovatele/subzpracovatele, s výjimkou případů, kdy se jedná o společnosti uvedené ve Specifikaci služby, resp. v Příloze č. 3 – *Schválení Dílčí zpracovatelé a Subdodavatelé Dílčích zpracovatelů*, nebo o společnosti v rámci skupiny Deutsche Telekom. Smluvní partner uděluje souhlas s využitím těchto subzpracovatelů. Zpracovatel informuje písemně (včetně e-mailu) Správce o veškerých zamýšlených změnách (přijetí/nahrazení), s tím, že Správce má právo vznést do 14 (čtrnácti) dnů vůči těmto změnám objektivní a odůvodněné námitky. Smluvní strany se výslovně dohodly, že v případě, že Správce bezdůvodně odmítá změnu, je Zpracovatel oprávněn ukončit poskytování Služby výpovědí bez výpovědní doby, aniž by Správci vznikl jakýkoliv nárok na finanční náhradu spojenou s takovým ukončením Služby.

Výmaz osobních údajů

- 1.21. V případě ukončení Specifikace služby je Správce oprávněn žádat od Zpracovatele vrácení osobních údajů a/nebo si kopii osobních údajů stáhnout ve lhůtě 30 kalendářních dnů od ukončení Specifikace služby. Pokud Správce o vrácení nepožádá, Zpracovatel osobní údaje vymaže, pokud právo Evropské unie nebo právní předpisy České republiky nevyžadují uložení daných osobních údajů.

Nezpracovaná (primární) data shromážděná a přenesená poskytovaným řešením z IT prostředí Správce a uložená v cloudu (např. protokoly z koncových zařízení a procesní data shromážděná Bezpečnostní platformou a agentem) jsou dočasně ukládána a po uplynutí stanovené doby automaticky odstraňována ze systémů. Vymazání dat jednotlivých modulů je v případě potřeby upraveno samostatně v popisu dané služby. Data jsou obvykle vymazána nejpozději po 90 dnech nebo dříve.

Bezprostředně po ukončení Služby budou osobní údaje Správce v Bezpečnostní platformě vymazány, pokud Poskytovatel není na základě právních předpisů povinen nebo vzhledem ke svému oprávněnému zájmu oprávněn uchovávat osobní údaje po delší dobu. V takovém případě budou tyto údaje vymazány po uplynutí příslušných lhůt.



2 **Ceník úkonů – součinnost zpracovatele**

Součinnost zpracovatele v souvislosti s požadavky správce podle čl. 1.16 těchto Podmínek (povinnost správce poskytnout informace orgánům státní správy, povinnost správce reagovat na žádost o uplatnění práv subjektu údajů,) se řídí níže uvedeným ceníkem.

Jiné ceníkové položky	Perioda zpoplatnění	Cena	Cena jednotky
Úkony související se zpracováním osobních údajů*			

„**započatá hodina**“ – cena je účtována, pokud Smluvní partner danou položku využil, kdykoliv v průběhu jedné standardní denní hodiny (hodina začínající vždy x:00 a končící vždy x:59, tj. 24 na sebe bezprostředně navazujících 60minutových intervalů v rámci kalendářního dne)

*První žádost Správce v kalendářním měsíci není zpoplatněna. Maximální cena za úkony Zpracovatele související se zpracováním jedné žádosti nepřesáhne cenu za 5MD (Man-Day).



Příloha č. 1 – Technická a organizační opatření

A. Důvěrnost (článek 32 odst. 1 písm. b Obecného nařízení EU na ochranu osobních údajů – GDPR)

Kontrola vstupu

Zabezpečení systémů pro zpracovávání údajů před přístupem neoprávněných osob, např. prostřednictvím magnetických nebo čipových karet, klíčů, elektrických otvíračů dveří, bezpečnostní služby a/nebo vrátného, alarmu, videosystémů apod.

Kontrola přístupu

Zabezpečení systémů před neoprávněným použitím, např. prostřednictvím (bezpečnostních) hesel, mechanismů automatického zamykání, dvouúrovňového ověřovacího mechanismu, šifrování nosičů údajů apod.

Kontrola přístupových oprávnění

Zabezpečení, aby osoby bez příslušného oprávnění nemohly údaje číst, kopírovat, upravovat či vymazávat, např. prostřednictvím autorizačních konceptů, přístupových práv na základě příslušných potřeb a evidence přístupů

B. Integrita (článek 32 odst. 1 písm. b GDPR)

Kontrola zpřístupňování údajů

Zabezpečení, aby v průběhu elektronického přenosu nebo přepravy nemohly osoby bez příslušného oprávnění tyto údaje číst, kopírovat, upravovat či vymazávat, např. prostřednictvím šifrování, virtuálních privátních sítí (VPN), elektronického podpisu apod.

Kontrola zadávání údajů

Zajištění, aby bylo možné zpětně ověřit a zjistit, zda a kým byly osobní údaje do systémů pro zpracovávání údajů zadány, upravovány nebo z těchto systémů vymazány, např. prostřednictvím evidence oprávnění, vedení záznamů o zadávání údajů apod.

C. Dostupnost a odolnost systémů (článek 32 odst. 1 písm. b GDPR)

Kontrola dostupnosti

Ochrana údajů před náhodným nebo úmyslným zničením a/nebo ztrátou, např. prostřednictvím zálohování (online/off-line; on-site/off-site), nepřerušitelných zdrojů napájení (UPS), antivirové ochrany, firewallů, zaznamenávání přenosových tras a krizových plánů

Schopnost obnovit dostupnost údajů (článek 32 odst. 1 písm. c GDPR)

D. Proces pravidelného testování, posuzování a hodnocení (článek 32 odst. 1 písm. d GDPR; článek 25 odst. 1 GDPR)

- Řízení ochrany údajů
- Řízení reakcí na incidenty
- Výchozí nastavení, která zajišťují ochranu údajů (článek 25 odst. 2 GDPR)
- Kontrola smluvní strany

Zákaz smluvního zpracovávání údajů ve smyslu článku 28 GDPR bez příslušných pokynů od zákazníka, např. jednoznačná smlouva, formální výběrové řízení, přísný výběr poskytovatele služeb, povinnost provádění důkladných kontrol předem a provádění následných kontrol



Příloha č. 2 - Specifikace zpracování

Účel zpracování

- Údaje budou zpracovávány pro účely plnění Služby definované ve Specifikaci služby.
- Zřízení a správa Služby, konzultace ke konfiguraci, zjištěným událostem a reakce na bezpečnostní incidenty.

Kategorie Subjektů údajů

- Uživatelé Služby Magenta EDR.

Kategorie údajů a jejich jednotlivé atributy (typy)

- Jsou zpracována zejména metadata o spuštěných souborech, vykonaných příkazech síťových spojení, přihlášených uživatelích a telemetrie Chráněných zařízení.

Zvláštní kategorie údajů

- ☒Nebude zpracovávána žádná kategorie citlivých údajů.
- ☐Budou zpracovávány následující kategorie citlivých údajů
 - ☐národnostní, rasový nebo etnickém původ
 - ☐politické postoje
 - ☐členství v odborových organizacích
 - ☐náboženství a filozofickém přesvědčení
 - ☐odsouzení za trestný čin
 - ☐zdravotní stav
 - ☐informace o sexuálním životě
 - ☐genetické údaje
 - ☐biometrické údaje

Místo zpracování údajů

- Evropská unie

Přístup k datům

- Správce poskytuje údaje/umožňuje Zpracovateli přístup k údajům nebo umožňuje Zpracovateli shromažďovat osobní údaje, jak je popsáno níže.
- Zpracovatel přistupuje k údajům prostřednictvím dálkového přístupu do cloudové služby nebo lokální počítačové aplikace.

Doba zpracování

- ☒po dobu nezbytně nutnou, max. po dobu trvání smluvního vztahu ke Službě.
- ☐po dobu nezbytně nutnou, maximálně po dobu



Příloha č. 3 – Schválení Dílčí zpracovatelé a Subdodavatelé

CrowdStrike, Inc, 150 Mathilda Place, Suite 300, Sunnyvale, California 94086, USA – poskytovatel cloudové technologie EDR a provozovatel Bezpečnostní platformy využívané při poskytování Služby. Jeho zpracování osobních údajů se řídí podmínkami zveřejněnými na www.crowdstrike.com.

Datové centrum CrowdStrike je umístěné na území EU.